

CyberTalents Challenges

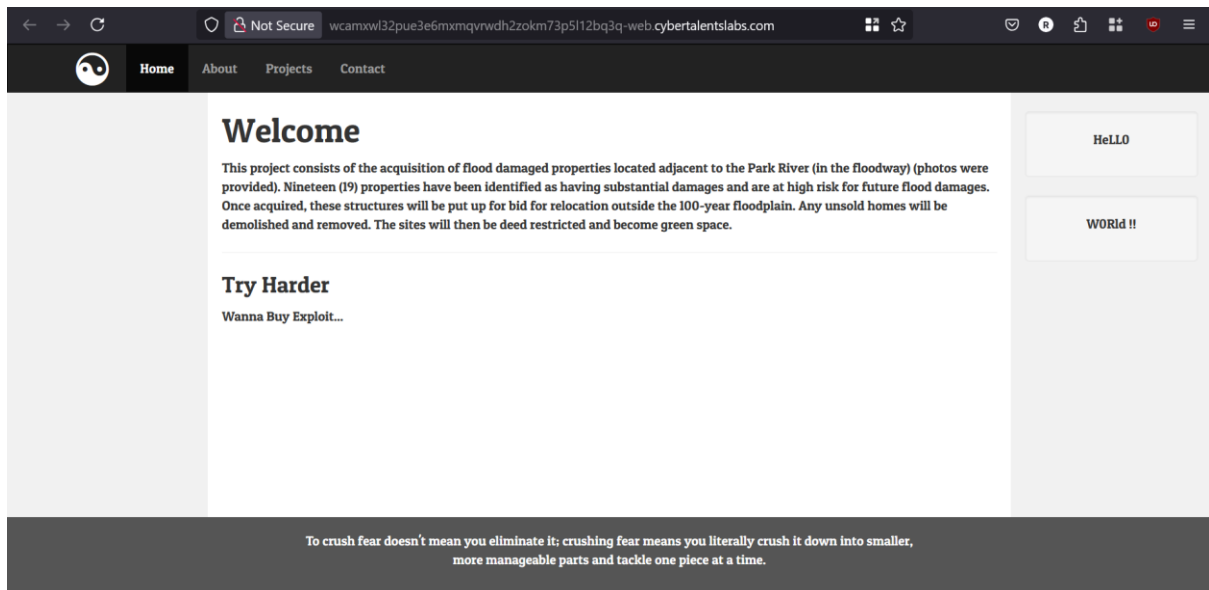
Web Security – catch me if you can – level medium

Author: levith4n

Description:

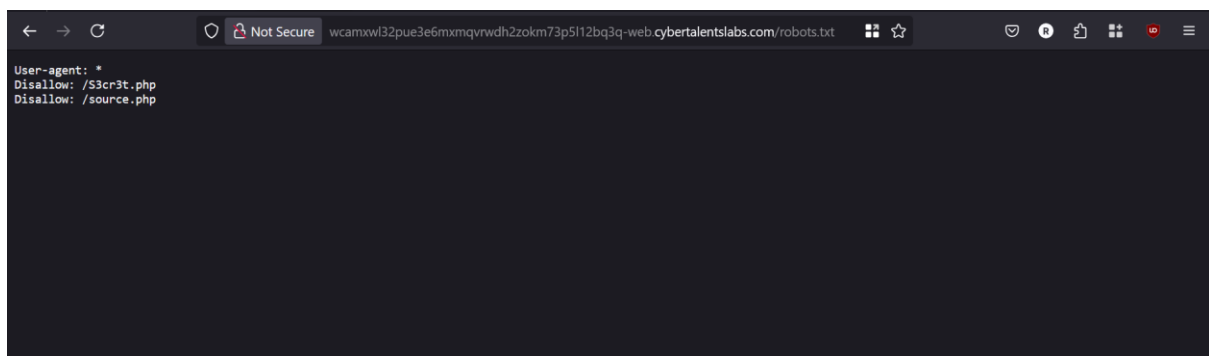
I'm Just wanna Make Sure if you Are Mr.Robot

Pertama, ini adalah tampilan utama website, saya mencoba untuk menelusuri halaman-halaman yang ada, ternyata semuanya hanyalah *fragment* saja.

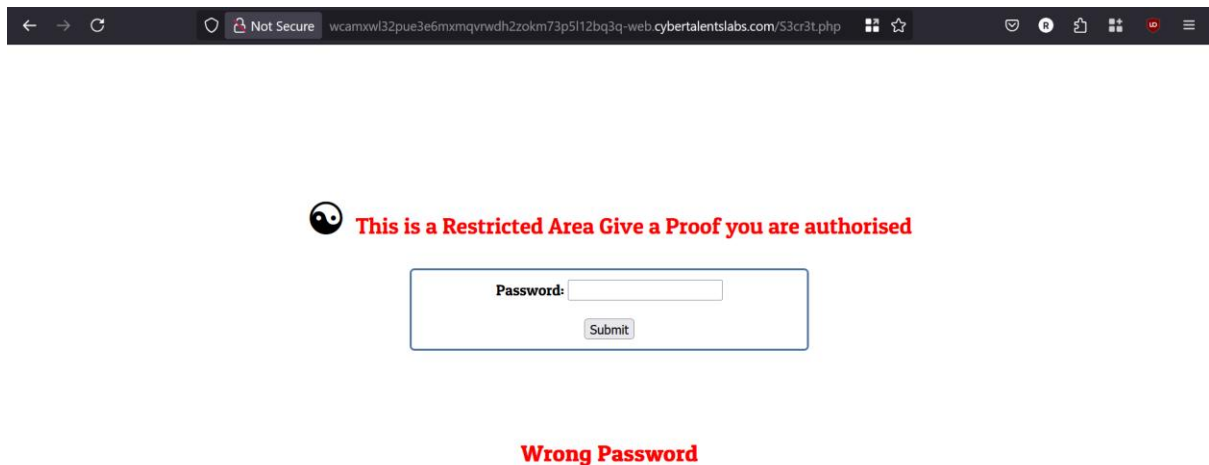


Kemudian, saya mencoba melakukan *information gathering* dengan mencoba membuka file **robots.txt**. Saya mendapatkan dua halaman, yaitu **/S3cr3t.php** dan **/source.php**.

Catatan: file robots.txt berfungsi sebagai petunjuk bagi bot atau crawler mesin pencari, seperti Googlebot, untuk mengontrol bagaimana mereka menjelajahi sebuah website



Kemudian, saya mencoba untuk mengunjungi kedua halaman tersebut. Pada halaman **/S3cr3t.php** saya menemukan sebuah form untuk memasukkan password.



The screenshot shows a web browser window with the address bar displaying "Not Secure" and the URL "wcamxwl32pue3e6mxmqvndh2zokm73p5l12bq3q-web.cybertalentslabs.com/S3cr3t.php". The main content area features a red warning message: "This is a Restricted Area Give a Proof you are authorised" next to a padlock icon. Below this is a form with a "Password:" label, a text input field, and a "Submit" button. At the bottom of the page, a red error message "Wrong Password" is displayed.

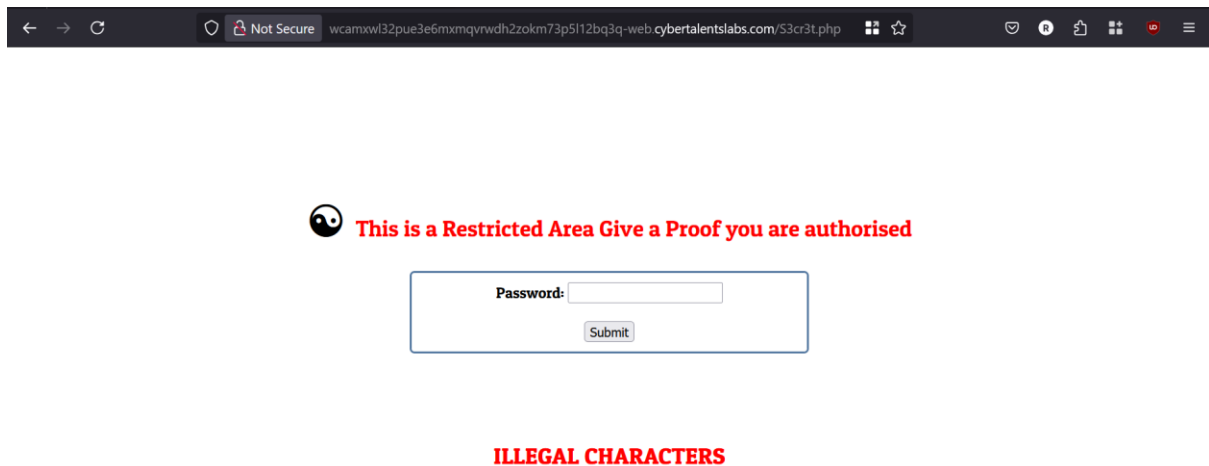
Lalu, halaman **/source.php** sepertinya *source code* dari halaman **/S3cr3t.php**. Pada *source code* saya melihat sebuah pengkondisian, jika password sama dengan **R_4r3@** maka kode akan dilanjutkan dan tidak berakhir dengan pesan "Wrong Password". Ketika kode dilanjutkan akan ada sebuah pengkondisian lagi yang memeriksa password yang dimasukkan dengan *regex*. Masalahnya, password **R_4r3@** tidak sama dengan pola *regex* yang ada pada *source code*, sehingga ini akan membuat kita mendapatkan pesan "ILLEGAL CHARACTERS" dan kode tidak dilanjutkan.



The screenshot shows a web browser window with the address bar displaying "Not Secure" and the URL "wcamxwl32pue3e6mxmqvndh2zokm73p5l12bq3q-web.cybertalentslabs.com/source.php". The main content area displays the PHP source code for the page:

```
<?php
include('flag.php');
$password=$_POST['pass'];
if (strpos( $password, 'R_4r3@')!== FALSE){
    if (!preg_match('/^-[a-z0-9]+$/', $password)) {
        die('ILLEGAL CHARACTERS');
    }
    echo $cipher;
}
else
{
    echo 'Wrong Password';
}
?>
```

Seperti yang ada pada *source code*, password **R_4r3@** yang akan membuat kita mendapatkan pesan “ILLEGAL CHARACTERS”.



The screenshot shows a web browser window with a dark theme. The address bar displays a long, random URL. Below the address bar, there is a red warning icon and the text "This is a Restricted Area Give a Proof you are authorised". In the center, there is a white rectangular box containing a "Password:" label, a text input field, and a "Submit" button. Below this box, the text "ILLEGAL CHARACTERS" is displayed in red.

Jika kita perhatikan, setelah pembatas terakhir terdapat *modifier m* (*multiline*) yang membuat pengecekan ini berlaku untuk setiap baris. Kita bisa memanfaatkan hal ini dengan membuat dua baris password, yaitu satu password yang valid dan yang tidak valid untuk mem-*bypass* *regex* ini.

```
if (!preg_match('/^-?[a-z0-9]+$/', $password)) {  
    die('ILLEGAL CHARACTERS');  
}
```

Pertama-tama, kita akan menambahkan password yang tidak valid seperti string “kocak”, password tidak valid ini digunakan untuk mem-*bypass regex*, selanjutnya kita menambahkan `%0a` atau *URL encoding* dari **newline** (`/n`). Setelah itu, kita menambahkan password yang valid `R_4r3@` untuk melewati pengecekan password yang valid.

Catatan: Tidak masalah apakah password yang valid atau tidak valid yang ada pada baris pertama, karena masing-masing pengecekan akan melakukan pencarian terhadap semua baris.

Seperti yang kita duga, kita berhasil mem-*bypass* hal ini dan mendapatkan sebuah kode **Brainfuck**.

The screenshot displays a web application security tool interface with two main panels: Request and Response.

Request Panel: Shows a POST request to `/S3cr3t.php` with the following details:

- Method: POST
- URL: `/S3cr3t.php`
- Host: `weanewl32pue2e6nmgvrwdh2sokm73p5112hq3q-web.cybertalentslabs.com`
- Cache-Control: `max-age=0`
- Accept-Language: `en-US,en;q=0.9`
- Origin: `http://weanewl32pue2e6nmgvrwdh2sokm73p5112hq3q-web.cybertalentslabs.com`
- Upgrade-Insecure-Requests: `1`
- User-Agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36`
- Accept: `text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7`
- Referer: `http://weanewl32pue2e6nmgvrwdh2sokm73p5112hq3q-web.cybertalentslabs.com/S3cr3t.php`
- Accept-Encoding: `gzip, deflate, br`
- Content-Type: `application/x-www-form-urlencoded`
- Content-Length: `19`
- Body: `pass=kocak%0aR_4r3@`


Response Panel: Shows the server's response, which includes a message and a password input form.

Message: "This is a Restricted Area Give a Proof you are authorised"

Form: A password input field with the label "Password:" and a "Submit" button.

Brainfuck Message: "Can You Read This For Me ?"

Brainfuck Code: A block of Brainfuck code is displayed below the message.



Search for a tool

* SEARCH A TOOL ON dCODE BY KEYWORDS:
 e.g. type "caesar"

* BROWSE THE FULL dCODE TOOLS LIST

Results

Input: `-[----->+<.>.`
 Arg:
 Output:

[L4g\(R35tr1C1d_Ar34\)](#)

Memory Dump: [index] = char (ASCII code)
 [0] = (0)
 [4] = R (82)
 [6] = 3 (51)
 [16] = r (114)
 [18] = 4 (52)
 [20] = } (125)
 pointer = 20
 Brainfuck - dCode
 Tag(s) : Programming Language

BRAINFUCK

Informatics • Programming Language • Brainfuck

BRAINFUCK INTERPRETER

* BRAINFUCK CODE TO INTERPRET

```

+<.>. [->+<.>.> [->+<.>.> [->+<.>.> [->+<.>.>
+.-.- [->+<.>.>.-.- [->+<.>.>.-.- [->+<.>.>.-.-
<.>.+<.>+<.>.-.-.-.-.+<.>+<.>+<.>.-.-.-.-.-.-.-.-
+<.>+<.>+<.>.-.-.-.-.+<.>+<.>+<.>.-.-.-.-.-.-.-.-
+<.>+<.>+<.>.-.-.-.-.+<.>+<.>+<.>.-.-.-.-.-.-.-.-

```

* ARGUMENT
 * SHOW MEMORY STATE ☒

EXECUTE

See also: Leet Speak 1337 – LOLCODE Language – ReverseFuck – Alphuck – JSFuck Language [!](if+[]) – Binaryfuck

BRAINFUCK ENCODER

* PLAINTEXT TO CODE IN BRAINFUCK

dCode Brainfuck

* ADD A SEPARATOR BETWEEN INSTRUCTIONS

ENCRYPT

Answers to Questions (FAQ)
 What is Brainfuck? (Definition)

Summary

- * Brainfuck Interpreter
- * Brainfuck Encoder
- * What is Brainfuck? (Definition)
- * How does Brainfuck work?
- * How to encrypt using Brainfuck code?
- * How to encrypt using Brainfuck Shortcut code?
- * How to decrypt Brainfuck code?
- * How to recognize Brainfuck coded text?
- * What is the memory state?
- * What are the variants of the Brainfuck code?
- * What is Brainfuck for?
- * When was Brainfuck invented?

Similar pages